

GETLOGIN

Results of getlogin() should not be trusted

Sean Barnum, Cigital, Inc. [vita¹]

Copyright © 2007 Cigital, Inc.

2007-03-23

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 4079 bytes

Attack Category	<ul style="list-style-type: none">• Identity Spoofing								
Vulnerability Category	<ul style="list-style-type: none">• Privilege escalation problem• Access Control								
Software Context	<ul style="list-style-type: none">• Authorization								
Location									
Description	<p>The results of <code>getlogin()</code> should not be trusted.</p> <p>The <code>getlogin()</code> function returns a pointer to a string that contains the name of the user associated with the calling process. The function is not reentrant, meaning that if it is called from another process, the contents are not locked out and the value of the string can be changed by another process. This makes it very risky to use because the username can be changed by other processes, so the results of the function cannot be trusted.</p> <p>Also, according to the Linux man page: "Unfortunately, it is often rather easy to fool <code>getlogin()</code>. Sometimes it does not work at all, because some program messed up the <code>utmp</code> file. Often, it gives only the first 8 characters of the login name. The user currently logged in on the controlling tty of our program need not be the user who started it. Avoid <code>getlogin()</code> for security-related purposes."</p> <p>Guidance: Using names for security purposes is not advised. Names are easy to forge and can have overlapping user IDs, potentially causing confusion or impersonation.</p>								
APIs	<table><tr><th>Function Name</th><th>Comments</th></tr><tr><td><code>getlogin</code></td><td></td></tr></table>			Function Name	Comments	<code>getlogin</code>			
Function Name	Comments								
<code>getlogin</code>									
Method of Attack									
Exception Criteria									
Solutions	<table><tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr><tr><td></td><td></td><td></td></tr></table>			Solution Applicability	Solution Description	Solution Efficacy			
Solution Applicability	Solution Description	Solution Efficacy							

1. http://buildsecurityin.us-cert.gov/bsi/about_us/authors/35-BSI.html (Barnum, Sean)

	<div>When login user name is needed.</div> <div>Never trust the results of the function <code>getlogin()</code>. Use <code>getlogin_r()</code> instead, which is reentrant, meaning that other processes are locked out from changing the username.</div> <div>Somewhat effective. Eliminates risk of buffer being overwritten, but other risks may persist.</div>				
Signature Details	<code>char *getlogin(void);</code>				
Examples of Incorrect Code	<pre>/* The following is not trustworthy */ char *userName = getlogin();</pre>				
Examples of Corrected Code	<pre>/* The following is more trustworthy, but still has possible issues */ const int userNameSize = L_cuserid; // Standard macro giving size of user names char userName[userNameSize]; if (getlogin_r(userName, userNameSize)) { handleError(); }</pre>				
Source Reference	<ul style="list-style-type: none"> Rough Auditing Tool for Security (RATS)² 				
Recommended Resource	<ul style="list-style-type: none"> Linux man page for <code>getlogin()</code>, <code>getlogin_r()</code>³ 				
Discriminant Set	<table> <tr> <td>Operating System</td><td> <ul style="list-style-type: none"> Windows </td></tr> <tr> <td>Languages</td><td> <ul style="list-style-type: none"> C C++ </td></tr> </table>	Operating System	<ul style="list-style-type: none"> Windows 	Languages	<ul style="list-style-type: none"> C C++
Operating System	<ul style="list-style-type: none"> Windows 				
Languages	<ul style="list-style-type: none"> C C++ 				

Cigital, Inc. Copyright

Copyright © Cigital, Inc. 2005-2007. Cigital retains copyrights to this material.

Permission to reproduce this document and to prepare derivative works from this document for internal use is granted, provided the copyright and “No Warranty” statements are included with all reproductions and derivative works.

For information regarding external or commercial use of copyrighted materials owned by Cigital, including information about “Fair Use,” contact Cigital at copyright@cigital.com¹.

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

1. <mailto:copyright@cigital.com>